PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Carl Rajsic
For	:	METHOD AND APPARATUS FOR SECURELY ESTABLISHING L3-SVC CONNECTIONS
Serial No.:	:	10/814,330
Filed	:	April 1, 2004
Art Unit	:	2619
Examiner	:	Michael J. Moore, Jr.
Att. Docket	:	ALC 3124
Confirmation No.	:	5344

APPEAL BRIEF

Mail Stop Appeal Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed herewith.

I. REAL PARTY IN INTEREST

The party in interest is ALCATEL, by way of an Assignment recorded at Reel 015165, frame 0097.

II. RELATED APPEALS AND INTERFERENCES

Following are identified any prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal:

NONE.

III. STATUS OF CLAIMS

Claims 1-13 are on appeal.

Claims 1-13 are pending.

No claims are allowed.

Claims 1-13 are rejected.

IV. STATUS OF AMENDMENTS

All Amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The subject matter recited in claim 1 relates to a method of establishing a secure Layer-3 connection across an ATM network (Page 4, paragraph 10, line 4; Figure 1:12), the Layer-3 connection having a first endpoint (Page 4, paragraph 10, lines 4-5; Figure 1:14) at an egress port (Page 4, paragraph 10, line 5; Figure 1:16) of an originating multiservice switch (MSS) (Page 4,

paragraph 10, lines 5-6; Figure 1:18) and a second endpoint (Page 4, paragraph 10, line 6; Figure 1:20) at an ingress port (Page 4, paragraph 10, line 6; Figure 1:22) of a terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24), the method comprising the steps of configuring the terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24) with anticipated security information; at the originating MSS (Page 4, paragraph 10, lines 5-6; Figure 1:18), generating a setup message including embedded security information (Page 7, paragraph 18, lines 5-6; Figure 2:62); sending the setup message to the terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24); at the terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24), extracting the embedded security information from the setup message (Page 9, paragraph 23, lines 2-4; Figure 3:90); determining whether the embedded security information matches the anticipated security information (Page 9, paragraph 24, lines 4-6; Figure 3:100); and if the embedded security information matches the anticipated security information, establishing the Layer-3 connection (Page 9, paragraph 24, line 6 and Page 10, paragraph 24, lines 1-2; Figure 3:102).

The subject matter recited in claim 10 relates to an originating multiservice switch (MSS) for establishing a secure Layer-3 connection across an ATM network (Page 4, paragraph 10, line 4; Figure 1:12) to a terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24), comprising a call control for generating a Layer-3 connection setup message including embedded security information (Page 7, paragraph 18, lines 5-6; Figure 2:62), and for sending the setup message to the terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24), wherein the embedded security information is compared with anticipated security information at the terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24).

The subject matter recited in claim 11 relates to a computer-readable medium encoded with a computer program, the computer program comprising: instructions for generating a Layer-3 connection setup message to be sent from an originating multiservice switch (MSS) (Page 4, paragraph 10, lines 5-6; Figure 1:18) to a terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24); and instructions for embedding security information within the setup message (Page 8, paragraph 20, lines 2-3; Figure 2:68), the security information compared with anticipated security information at the terminating MSS (Page 4, paragraph 10, line 7; Figure 1:24).

The subject matter recited in claim 12 relates to a terminating multiservice switch (MSS) (Page 4, paragraph 10, line 7; Figure 1:24) for establishing a secure Layer-3 connection across an ATM network (Page 4, paragraph 10, line 4; Figure 1:12) from an originating MSS (Page 4, paragraph 10, lines 5-6; Figure 1:18), comprising: stored anticipated security information (Page 8, paragraph 20, lines 2-3; Figure 2:68); means for querying a comparator of two pieces of security information (Page 9, paragraph 24, lines 2-3, Figure 3:98); and a call controller for receiving a Layer-3 connection setup message (Page 8, paragraph 21, lines 4-5, Figure 3:80), for extracting embedded security information from the setup message (Page 9, paragraph 23, lines 2-4; Figure 3:90), for querying the comparator to determine whether the embedded security information corresponds to the anticipated security information (Page 9, paragraph 24, lines 4-6; Figure 3:100), and for establishing the Layer-3 connection in the event that the embedded security information corresponds to the anticipated security information (Page 9, paragraph 24, line 6 and Page 10, paragraph 24, lines 1-2; Figure 3:102).

The subject matter recited in claim 13 relates to a computer-readable medium encoded with a computer program, the computer program comprising: instructions for receiving a Layer-3 connection setup message received from an originating multiservice switch (Page 4, paragraph 10, lines 5-6; Figure 1:18); instructions for extracting embedded security information from the setup message (Page 9, paragraph 23, lines 2-4; Figure 3:90); instructions for retrieving anticipated security information (Page 9, paragraph 23, line 8; Figure 3:96); instructions for determining whether the embedded security information corresponds to the anticipated security information (Page 9, paragraph 24, lines 2-3, Figure 3:98); and instructions for establishing a Layer-3 connection in the event that the embedded security information corresponds to the anticipated security information (Page 9, paragraph 24, lines 4-6; Figure 3:100).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are presented for review:

A. Claims 1, 4, 5, 7, and 9-13 are rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 7,130,393 to Hall, Jr. et al. (hereinafter "Hall").

B. Claims 2 and 3 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hall in view of U.S. Published Application No. 2002/0064159 to Shirakawa (hereinafter "Shirakawa").

C. Claims 6 and 8 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hall in view of U.S. Patent No. 6,757,278 to Bi et al. (hereinafter "Bi").

VII. ARGUMENT

A. Rejection of Claims 1, 4, 5, 7, and 9-13 Under 35 U.S.C. § 102(e)

In section 3 on pages 2-8, the Final Office Action, dated January 8, 2008, rejects claims 1, 4, 5, 7, and 9-13 under 35 U.S.C. § 102(e) as allegedly being anticipated by Hall.

The test for anticipation under section 102 is whether each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ.2d 1051, 1053 (Fed. Cir. 1987); M.P.E.P. § 2131. The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ.2d 1913, 1920 (Fed. Cir. 1989); M.P.E.P. § 2131. The elements must also be arranged as required by the claim. *In re Bond*, 15 USPQ.2d 1566 (Fed. Cir. 1990).

1. Claim 1

Independent claim 1 recites a step of "configuring the terminating MSS with anticipated security information" (emphasis added). As disclosed in paragraph [17] of the specification, the terminating MSS 24 is configured with anticipated security information before establishment of a secure Layer-3 SPVC is attempted. This security information is related in the configuration to a call setup scenario.

With respect to the above-quoted subject matter, page 3 of the Office Action relies upon lines 57-59 in column 19 in Hall. The Office Action alleges that closed user group identifiers correspond to the above quoted subject matter. Page 10 of the Office Action further alleges that these identifiers can be considered "anticipated security information" because a calling party closed user group identifier corresponding to a called party closed user group identifier is expected to be found in order to establish a connection, referring to lines 1-22 of column 20 in Hall.

However, Hall clearly does not select only "anticipated" closed user group identifiers. As recited on lines 48-50 of column 19, all closed group identifiers for the calling party, or calling user, are retrieved. Thus, Hall cannot select only a subset of the identifiers based upon whether they are "anticipated" to correspond to security information.

Moreover, Hall does not "configure" a terminating MSS with anticipated security information. Page 10 of the Office Action alleges that MSCP 44 in Hall is equivalent to the claimed terminating MSS. However, Hall is silent regarding any configuration of MSCP 44 with anticipated security information. Instead, as depicted in Fig. 5, Hall's method includes steps of

retrieving all CUG identifiers associated with both the calling [504] and called [506] parties. Thus, Hall does not configure a terminating MSS with anticipated security information.

Accordingly, Hall does not disclose, teach, or suggest the step of "configuring the terminating MSS with anticipated security information," as recited in claim 1.

For at least the forgoing reasons, claim 1 is patentable over Hall because Hall fails to disclose, teach, or suggest each and every element recited in claim 1.

2. Claims 10, 11, and 13

Independent claims 10 and 11 recite "embedded security information "compared with anticipated security information at the terminating MSS" (emphasis added). Independent claim 13 determines "whether the embedded security information corresponds to the anticipated security information," (emphasis added). As disclosed in paragraph [24] of the specification, the call controller sends the embedded security information and the anticipated security information to the comparator. The comparator then compares the two sets of security information and returns a comparison result to the call controller.

Page 3 of the Office Action alleges that step 508 of Fig. 5 in Hall anticipates the above-quoted subject matter. The Office Action also refers to determination of whether a closed user group identifier (security information) that is common (match) to both the calling and called parties, as recited in lines 1-22 of column 20 in Hall.

However, step 508 of Fig. 5 clearly does not involve a comparison of anticipated and embedded security information. Instead, it is evident that Hall retrieves all CUG identifiers associated with both the calling and called parties. Thus, rather than efficiently comparing only

anticipated security information to retrieved embedded security information, Hall inefficiently compares all security information, because Hall's system lacks a terminating MSS that is configured to anticipate which security information may be embedded in a future call.

Accordingly, Hall does not disclose, teach, or suggest either comparing embedded security information to "anticipated security information at the terminating MSS," as recited in claims 10 and 11, or whether it "corresponds to the anticipated security information," as recited in claim 13.

For at least the forgoing reasons, claims 10, 11, and 13 are patentable over Hall because Hall fails to disclose, teach, or suggest each and every element recited in claims 10, 11, and 13.

3. Claim 12

Independent claim 12 recites "a terminating multiservice switch (MSS) . . . comprising: stored anticipated security information" (emphasis added). As disclosed in paragraph [17] of the specification, the terminating MSS 24 is configured with anticipated security information before establishment of a secure Layer-3 SPVC is attempted. This security information is related in the configuration to a call setup scenario.

With respect to the above-quoted subject matter, page 6 of the Office Action relies upon lines 57-59 in column 19 in Hall. The Office Action also alleges that closed user group identifiers correspond to the above quoted subject matter. Page 10 of the Office Action further alleges that these identifiers can be considered "anticipated security information" because a calling party closed user group identifier corresponding to a called party closed user group identifier is expected to be found in order to establish a connection, referring to lines 1-22 of column 20 in Hall.

However, Hall clearly does not select only "anticipated" closed user group identifiers. As recited on lines 48-50 of column 19, all closed group identifiers for the calling party, or calling user, are retrieved. Thus, Hall cannot select only a subset of the identifiers based upon whether they are "anticipated" to correspond to security information.

Moreover, Hall does not "configure" a terminating MSS with anticipated security information. Page 10 of the Office Action alleges that MSCP 44 in Hall is equivalent to the claimed terminating MSS. However, Hall is silent regarding any configuration of MSCP 44 with anticipated security information. Instead, as depicted in Fig. 5, Hall's method includes steps of retrieving all CUG identifiers associated with both the calling [504] and called [506] parties. Thus, Hall does not configure a terminating MSS with anticipated security information.

Accordingly, Hall does not disclose, teach, or suggest "stored anticipated security information," as recited in claim 12.

For at least the forgoing reasons, claim 12 is patentable over Hall because Hall fails to disclose, teach, or suggest each and every element recited in claim 12.

4. Claim 4

Claim 4 depends from claim 1 and is therefore allowable for at least the reasons stated above in connection with claim 1, as well as for the separately patentable subject matter described in detail below.

Claim 4 recites "wherein the embedded security information and the anticipated security information are Closed User Group Interlock Codes" (emphasis added). As disclosed in paragraph

[14] of the specification, the setup message includes security information, such as a Closed User Group (CUG) Interlock Code (IC).

Page 4 of the Office Action alleges that the above-quoted subject matter is anticipated by the calling party and called party closed used group identifiers, referring to lines 48-56 of column 19 in Hall. The Office Action is silent regarding interlock codes.

A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. *In re Kahn*, 441 F.3d 977, 990 (Fed. Cir. 1996); *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994).

In this case, it is evident that Hall teaches away from the use of interlock codes. First, on lines 36-48 of column 3, Hall teaches that interlock codes are not defined. Second, on lines 20-22 of column, Hall's invention is defined as having the capability to provide closed user groups with VtoA without using an interlocking code. Third, on lines 34-36 of column 19, Hall recites advanced closed user group functionality, without the need or requirement of an interlocking code. Thus, it is clearly erroneous for the Office Action to allege that Hall's closed user groups use interlock codes.

Accordingly, Hall does not disclose, teach, or suggest "wherein the embedded security information and the anticipated security information are Closed User Group Interlock Codes," as recited in claim 4.

For at least the forgoing reasons, claim 4 is patentable over Hall because Hall fails to disclose, teach, or suggest each and every element recited in claim 4.

5. Claims 5, 7, and 9

Claims 5, 7, and 9 depend from claim 1 and are therefore allowable for at least the reasons stated above in connection with claim 1, as well as for the separately patentable subject matter recited therein.

B. Rejection of Claims 2 and 3 Under 35 U.S.C. § 103(a)

In section 5 on pages 8-9, the Final Office Action, dated January 8, 2008, rejects claims 2 and 3 under 35 U.S.C. § 103(a) as allegedly being anticipated by Hall in view of Shirakawa.

Claims 2 and 3 depend from claim 1 and are therefore allowable for at least the reasons stated above in connection with claim 1, as well as for the separately patentable subject matter recited therein. Shirakawa fails to remedy the deficiencies of Hall discussed above in connection with the rejection of claim 1.

C. Rejection of Claims 6 and 8 Under 35 U.S.C. § 103(a)

In section 6 on page 9, the Final Office Action, dated January 8, 2008, rejects claims 6 and 8 under 35 U.S.C. § 103(a) as allegedly being anticipated by Hall in view of Bi.

Claims 6 and 8 depend from claim 1 and are therefore allowable for at least the reasons stated above in connection with claim 1, as well as for the separately patentable subject matter recited therein. Bi fails to remedy the deficiencies of Hall.

CONCLUSION

For at least the reasons discussed above, it is respectfully submitted that the rejections are in error and that claims 1-13 are in condition for allowance. For at least the above reasons, Appellants respectfully request that this Honorable Board reverse the rejections of claims 1-13.

Respectfully submitted,
KRAMER & AMADO, P.C.

April 11, 2008
Date

Terry W. Kramer
Reg. No. 41,541

KRAMER & AMADO, P.C.
1725 Duke Street, Suite 240
Alexandria, VA 22314
Tel. (703) 519-9801
Fax. (703) 519-9802

VIII. CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL:

1. (Original) A method of establishing a secure Layer-3 connection across an ATM network, the Layer-3 connection having a first endpoint at an egress port of an originating multiservice switch (MSS) and a second endpoint at an ingress port of a terminating MSS, the method comprising the steps of:

configuring the terminating MSS with anticipated security information;

at the originating MSS, generating a setup message including embedded security information;

sending the setup message to the terminating MSS;

at the terminating MSS, extracting the embedded security information from the setup message;

determining whether the embedded security information matches the anticipated security information; and

if the embedded security information matches the anticipated security information, establishing the Layer-3 connection.

2. (Original) The method of claim 1 wherein the Layer-3 connection is a Soft Permanent Virtual Circuit, and wherein the embedded security information and the anticipated security information are associated with the first endpoint.

3. (Original) The method of claim 1 wherein the Layer-3 connection is a Soft Permanent Virtual Circuit, and wherein the embedded security information and the anticipated security information are associated with the second endpoint.

4. (Original) The method of claim 1 wherein the embedded security information and the anticipated security information are Closed User Group Interlock Codes.

5. (Original) The method of claim 1 wherein the Layer-3 connection is established by an originating user belonging to a configured set of originating users, and wherein the embedded security information and the anticipated security information are associated with the configured set of originating users.

6. (Original) The method of claim 1 wherein the Layer-3 connection is established through an Internet Protocol (IP) interface address at the originating MSS belonging to a set of configured IP interface addresses, and wherein the embedded security information and the anticipated security information are associated with the configured set of IP interface addresses.

7. (Original) The method of claim 1 wherein the Layer-3 connection is established to a terminating user belonging to a configured set of terminating users, and wherein the embedded security information and the anticipated security information are associated with the configured set of terminating users.

8. (Original) The method of claim 1 wherein the Layer-3 connection is established through an Internet Protocol (IP) interface address at the terminating MSS belonging to a set of configured IP interface addresses, and wherein the embedded security information and the anticipated security information are associated with the configured set of IP interface addresses.

9. (Original) The method of claim 1 comprising the further steps of:

at the originating MSS, setting a value of a flag in the setup message to indicate that the setup message includes embedded security information;

at the terminating MSS, reading the value of the flag before extracting the embedded security information.

10. (Previously Presented) An originating multiservice switch (MSS) for establishing a secure Layer-3 connection across an ATM network to a terminating MSS, comprising a call control for generating a Layer-3 connection setup message including embedded security information, and for sending the setup message to the terminating MSS, wherein the embedded security information is compared with anticipated security information at the terminating MSS.

11. (Previously Presented) A computer-readable medium encoded with a computer program, the computer program comprising:

instructions for generating a Layer-3 connection setup message to be sent from an originating multiservice switch (MSS) to a terminating MSS; and

instructions for embedding security information within the setup message, the security information compared with anticipated security information at the terminating MSS.

12. (Original) A terminating multiservice switch (MSS) for establishing a secure Layer-3 connection across an ATM network from an originating MSS, comprising:

stored anticipated security information;

means for querying a comparator of two pieces of security information; and

a call controller for receiving a Layer-3 connection setup message, for extracting embedded security information from the setup message, for querying the comparator to determine whether the embedded security information corresponds to the anticipated security information, and for establishing the Layer-3 connection in the event that the embedded security information corresponds to the anticipated security information.

13. (Previously Presented) A computer-readable medium encoded with a computer program, the computer program comprising:

instructions for receiving a Layer-3 connection setup message received from an originating multiservice switch;

instructions for extracting embedded security information from the setup message;

instructions for retrieving anticipated security information;

instructions for determining whether the embedded security information corresponds to the anticipated security information; and

instructions for establishing a Layer-3 connection in the event that the embedded security information corresponds to the anticipated security information.

IX. EVIDENCE APPENDIX

A copy of the following evidence 1) entered by the Examiner, including a statement setting forth where in the record the evidence was entered by the Examiner, 2) relied upon by the Appellant in the appeal, and/or 3) relied upon by the Examiner as to the grounds of rejection to be reviewed on appeal, is attached:

NONE

X. RELATED PROCEEDINGS APPENDIX

Copies of relevant decisions in prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal are attached:

NONE